(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 September 2004 (02.09.2004)

PCT

(10) International Publication Number
WO 2004/075525 A1

(51) International Patent Classification[7]: H04M 15/00, G06F 1/14, H04Q 7/32, H04M 1/725, G07C 1/10

(21) International Application Number:
PCT/BE2004/000023

(22) International Filing Date: 20 February 2004 (20.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/BE03/00030 20 February 2003 (20.02.2003) BE
PCT/BE03/00075 30 April 2003 (30.04.2003) BE

(71) Applicant *(for all designated States except US)*: **ASE R & D Europe** [BE/BE]; Westerring 2, B-3600 Genk (BE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **PEIRSMAN, Bert** [BE/BE]; Hasseltweg 505 bus 21, B-3600 Genk (BE).

(74) Agents: **LUYS, Marie-José** et al.; Gevers & Vander Haeghen, Holidaystraat 5, B-1831 Diegem (BE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR OFFERING TIME ON SMART CARD AND METHOD FOR TIME REGISTRATION BY MEANS OF MOBILE COMMUNICATION DEVICE

(57) Abstract: A method for offering time on a smart card which is provided for being carried in a host device which comprises at least a first time counter and a gateway for communication with a time server. The method comprises the step of running an algorithm on a processor of the smart card for performing the following steps: reserving a user-inaccessible memory location on the smart card for storing a time; sending a synchronisation time request via the gateway to the time server and, upon receipt of a reply of the time server, extracting a synchronisation time from the reply and storing the synchronisation time as a reference time on the user-inaccessible memory location; starting the first time counter of the host device for counting an elapsed time with respect to the reference time; upon receipt of a present time request, retrieving the elapsed time from the first time counter, calculating a present time on the smart card by adding the elapsed time to the reference time and outputting the present time.

WO 2004/075525 A1

Method for offering time on smart card and method for time registration by means of mobile communication device

The present invention relates to a method for offering time on a smart card according to the preamble of claim 1. The invention further relates to a method for time registration by means of a mobile communication device according to the preamble of claim 14.

Devices which are provided for hosting a smart card and on which a time is offered, are known. An example of such a device is a cellular phone, in which the smart card is formed by the so-called SIM (Subscriber Identity Module) card. Presently, the time which is available on mobile phones, is provided by a user-accessible on-board clock. The time of this clock can be set and changed by the user. As a result, this time is unsuitable for use in applications where a trustable time is desired.

An application where a trustable time is desired is for example time registration by means of a cellular phone. A method for time registration by means of a cellular phone is for example known from WO-A-01/37225. In a first step of the time registration method known from WO-A-01/37225, the user's cellular phone communicates with a time data collecting unit for retrieving a series of task titles of tasks to be performed by the user. Upon starting work on a task, the user selects the task title on his cellular phone and a starting point is attached to the selected task title. This starting point and task title are then communicated to the computer unit, which stores the data in a database. When the user deselects the task title on the cellular phone or selects a different task, an ending point is attached to the task title and communicated to the computer unit. From the difference between the ending point and the starting point in time, it is calculated how much time the user has spent on the task.

It is nowhere described in WO-A-01/37225 how trustability of the time data collected on the time data collecting unit is or can be ensured. More particularly, there is no mention nor teaching in WO-A-01/37225 of how a trustable time can be offered on the cellular phone.

From WO-A-99/41919, a smart card is known which is provided with an integrated clock for providing a trustable time. By means of the integrated clock, an elapsed time is kept for billing purposes. The integrated clock is synchronised to an external clock signal, which is provided by the host device carrying the smart card.

The way in which time is provided on the smart card according to WO-A-99/41919 has the disadvantage that additional hardware needs to be present on the smart card. More particularly, an interface is needed via which the clock signal of the host device is passed on to the smart card and, since the frequency of external clock signals varies from one host device to another, measurement means are needed for measuring the frequency of the external clock signal.

It is an aim of the present invention to provide a method for offering a trustable time on a smart card with which the need for additional hardware on the smart card can be avoided.

This aim is achieved according to the invention with the method comprising the steps of the characterising part of claim 1.

It is further an aim of the invention to provide a method for time registration by means of a mobile communication device with which the trustability of the collected time data can be enhanced.

This aim is achieved according to the invention with the method comprising the steps of the characterising part of claim 14.

The method for offering time according to the invention is adapted for offering time on smart cards which are provided for being carried in a host device. This device forms a gateway for communication between the smart card and a time server. With the method of the invention, time is kept by using the memory which is provided on smart cards. According to international standards, the memory of the smart card is provided for storing given data, depending on the type of smart card or its application.

It is currently not provided in international standards to include a clock function on smart cards. According to the invention, such a clock function is applied to the smart card by means of an algorithm which is embedded on the smart card and is provided for performing the following steps:

a) reserving a user-inaccessible memory location on the smart card for storing a time,

b) sending a synchronisation time request via the gateway to the time server and, upon receipt of a reply of the time server, extracting a synchronisation time from the reply and storing the synchronisation time as a reference time on the user-inaccessible memory location,

c) starting a first time counter of the host device for counting an elapsed time with respect to the reference time,

d) upon receipt of a present time request, retrieving the elapsed time from the time counter, calculating a present time on the smart card by adding the elapsed time to the reference time and outputting the present time.

From the prior art, it is known to provide a clock function on a device which hosts a smart card, such as for example a cellular phone. This type of clock can be set and adjusted at will by the user to any given time. In other words, this clock is user-accessible. As a result, the time which is provided on the device in this way is unsuitable for applications where a trustable time is desired.

According to the invention, the time is kept by means of an algorithm which runs on the processor of the smart card. This algorithm makes user of a user-inaccessible space in the memory of the smart card for storing a reference time. Due to this inaccessibility towards the user, adjustment by the user of the reference time which is stored in the smart card memory can be prevented. In other words, according to the invention, time is kept without interaction with the user. As a result, a high trustability of the present time, which is calculated and outputted in step d), can be achieved with the method of the invention.

For keeping the time which is elapsed since the last synchronisation, the algorithm activates a time counter of the host device, which is for example a time counter of the SIM toolkit of a cellular phone. Using the time counter of the host device, whose time reading can normally be expected to

be correctly synchronised to the clock frequency of the host device, not only the need for an embedded time counter on the smart card can be avoided, but also the need for embedded clock frequency measurement means for achieving a correct time reading by such an embedded time counter. This shows that with the method of the invention the need for additional hardware on the smart card is avoided, so that the method of the invention can be applied on standard, presently available smart cards.

Furthermore, with the method of the invention, a trustable time can be kept on the smart card without requiring a continuous connection with the time server, i.e. the time is kept by means of an "offline clock" instead of an "online clock". The method of the invention only requires a connection for synchronisation (or re-synchronisation after a relatively long period of time), so that the need of a continuous or frequent connection with the time server can be avoided. Furthermore, since the synchronisation is triggered by the algorithm running on the smart card, monitoring of the time on the smart card by the time server can be avoided and the interaction between the smart card and the time server can be minimised. As a result, the algorithm of the method of the invention can function substantially independently on the smart card.

The time which is offered by means of the method of the invention is intended for use in any applications running on the smart card, on the host device or on an external device which is linked to the host device. Each time a valid time request is issued by such an application to the algorithm running on the smart card, the present time is calculated and outputted for use by the requesting application.

The method of the invention preferably further comprises the steps of encrypting the synchronisation time before it is sent from the time server to the smart card and decrypting the synchronisation time on the smart card. This encryption can further enhance the trustability of the present time which is calculated in the end.

The present time is preferably outputted in a time stamp which is generated on the smart card and comprises user-identification data which is stored on the smart card, document trustability data supplied by an application running on the host device (e.g. a hash value, a token or other), or

even any other data. In this way, the present time can be used for adding a trustability factor to the data to which it is linked in the time stamp.

The method of the invention preferably comprises the step of performing a validity check on the time request, before outputting the present time. This is to ensure that the present time or time stamp is only forwarded to authorities which have been authorised for performing a time request to the smart card.

The method of the invention preferably further comprises the step of checking the synchronisation time which is received from the time server for accuracy. Since the present time is calculated from the elapsed time with respect to the synchronisation time, this accuracy check may further enhance the trustability of the present time, which is calculated and outputted on request.

In a preferred embodiment of the method of the invention, preferably a second time counter is started simultaneously with the first time counter. In other words, both the first and second time counters count the elapsed time with respect to the reference time. The second time counter has a shorter duration than the first time counter. When this second time counter lapses, the first counter is restarted and the previously elapsed time, which is counted on the first counter, is added to the reference time and stored in the memory of the smart card as a new reference time. Afterwards, the present time is calculated on the basis of this new reference time. In this embodiment, the second time counter is used to obtain a warning signal that the first time counter is about to lapse. This warning signal is useful, since the operation of the smart card is mostly subordinate to the operation of the host device. It could for example occur that the first time counter lapses on a moment where the operation of the smart card is interrupted, due to the device being occupied with a different task. In this case, it could take some time before the first time counter can be restarted, which time would not be counted. This problem is obviated by means of the second time counter of shorter duration than the first, which serves to obtain that the first time counter can be restarted before it has lapsed.

The present time which is offered to the device by the method of the invention may be in the format of an absolute or universal standard time, such as for example UTC time, from which the current time and

date can be determined for each time zone, or already in the format of the date and time of the time zone where the device is located. To this end, the method of the invention preferably comprises steps for maintaining a time zone value and/or a daylight saving time flag in the memory of the smart card. The time zone value is determined by means of the synchronisation time, which is retrieved from the time server. This time zone value is forwarded to the device along with the present time on the occurrence of a time request, so that the value provides information on the time zone and can be used for showing the present time according to the respective time zone if desired, without affecting the reference time. The daylight saving time flag is set to a first value for winter time and a second value for summer time, for example "0", respectively "1". The present time is then adjusted in response to the value of the daylight saving time flag, for example by adding/subtracting one hour, depending on the case and if necessary. Further steps may be included in the method of the invention for taking leap years into account.

The gateway of the device which hosts the smart card can be provided for wireless communication as well as wired communication. In the case of wireless communication, the synchronisation time can for example be retrieved by sending an SMS (Short Message Service) message from the device via the wireless network to a network time server, which is incorporated in the wireless network of the operator, and via the wireless network back to the device. Alternatively, the synchronisation time may also be retrieved from a third party time server via wireless communication, such as for example the SMS protocol. SMS is preferred for economical reasons and simplicity of implementation, but any other wireless protocol known to the person skilled in the art may also be used.

In the case of wired communication, the synchronisation time is for example retrieved from the time server by means of a TCP/IP connection, but any other wired communication protocol known to the person skilled in the art may also be used.

The method for time registration according to the invention is adapted for enabling a user to register time points (points in time) to a time data collecting unit by means of a mobile telecommunication device, such as for example a cellular phone, a laptop provided with a telecommunication card

or other. The time points which are communicated from the telecommunication device to the time data collecting unit are calculated by means of the method described above. Preferably, wireless communication is used for retrieving the synchronisation time from the time server and communicating the time points to be registered to the time data collecting unit. More preferably, the SMS protocol is used in both cases. However, both communications may also involve any other form of wireless communication, such as for example a wireless call, WAP, GPRS, UMTS or other, or wired communication, such as for example a TCP/IP (transmission control protocol / internet protocol) connection, or other.

In the method for time registration according to the invention, a time point which is to be registered is preferably calculated on request, i.e. on operation of time registration means by the user via the user interface of the mobile telecommunication device. These time registration means, which are for example formed by a time registration algorithm comprising the steps for retrieving the present time and forwarding it to the time data collecting unit, are preferably also provided on the smart card, so that their security can be ensured. Alternatively, the time registration means may also be provided on the device itself. It is stressed that the calculation of the present time however occurs on the smart card.

In case of absence of connection between the device and the time data collecting unit, the time point to be registered is preferably stored on the smart card and communicated to the time data collecting unit once the connection is repaired.

The method for time registration according to the invention preferably further comprises the step of attaching user identification data to the time point which is communicated to the time data collecting unit. In this way, the time points can be allocated to different users, enabling a time registration system for a plurality of users.

The method for time registration according to the invention preferably further comprises steps for enabling the user to attach a task to the time point which is registered. These steps comprise the providing of task referencing means, e.g. in the time registration algorithm, by means of which the user can select a task reference or input a task reference for attachment to the time point. In the case of selection of the task reference, a series of task

references are preferably downloaded to the smart card in a previous step, for example in an initial communication between the time data collecting unit and the telecommunication device.

The method for time registration according to the invention preferably further comprises steps for attaching location information to the time point which is registered. The location information is retrieved from the telecommunication network. The use of location information may further enhance the trustability of the collected time data.

The invention will be further elucidated by means of the following description and the appended figures.

Figure 1 shows a schematic representation of a preferred embodiment of the method for offering time on a smart card according to the invention.

Figure 2 shows a preferred embodiment of the time synchronisation algorithm of figure 1.

Figure 3 shows a preferred embodiment of the time keeping algorithm of figure 1.

Figure 4 shows a preferred embodiment of the time stamping algorithm of figure 1.

Figure 5 shows a preferred embodiment of an algorithm for the time registration method of the invention.

The scheme of figure 1 shows that the invention relates to a generic method, designed to offer time on a smart card 3 for use in an application 4 running on the smart card 3, an application 5 running on a host device 2 which carries the smart card 3 or an external application 6 which communicates with the smart card 3 via the gateway 21 of the device 2. Providing the time on the smart card 3 itself has the advantage that, due to the nature of the smart card, this time and possible other data generated on the smart card and attached to the time is given the same level of security and authenticity as other information which is stored on the smart card 3 and other applications which may be provided on the smart card 3.

The smart card 3 can for example be the SIM (Subscriber Identity Module) card, which is used in mobile communications as a security and authentication tool, or a card for secure access to physical

networks, to virtual networks through PCs and set-top boxes and to secure transactions from any terminal. The time which is offered by the method of the invention can, due to the trustability achievable, be used in a wide variety of services and applications. Since the currently available smart cards do not have an embedded clock, an alternative mechanism to offer time is proposed. It is based on three components: a time server 1, a device 2 that can host the smart card 3 and the smart card 3 itself. The smart card 3 and device 2 may also be specifically designed for the sole purpose of providing a device by means of which a trustable/secure time stamp can be obtained, in which case the device 2 can for example be a card holder/reader for hosting for example a prepaid smart card 3 which is provided for supplying a predetermined number of time stamps to the device 2 on request.

The time server 1, from which the synchronisation time is retrieved, can be any time provider who is considered as acceptable for the target application or end user. Examples of such time servers are, but not exclusively, the mobile operators SMS-C (SMS service Center), an NTS (Network Time Server) or a TTA (Trusted Time Authority) such as for example the eTiming time server of the applicant. The synchronisation time which is supplied may be encrypted and/or accompanied by a certificate of the time provider, so that the time which is offered on the smart card 3 can be seen as having a certified trustability.

The device 2 comprises at least a smart card interface which is connected to a counter-system 22 and a gateway 21. Examples of such devices are, but not exclusively, any smart card reader connected or embedded to a PC or a laptop, a stand alone terminal with smart card reader, a cellular phone or other.

The gateway 21 offers the smart card algorithms the possibility of communication with external devices, such as for example the time server 1. Examples of such gateways are, but not exclusively, the SIM Toolkit on the GSM Phase2+ enabled mobile phones or a windows driver that enables the smart card to establish a TCP/IP connection via the internet with the time server 1. Additionally, the gateway 21 can offer access to external applications 6.

The counter-system 22 provides the algorithms on the smart card the means for keeping the time. The counter-system 22 typically has one counter and one timer, or two counters. For keeping the time, the counter-system 22 is started and its value is later on read for calculating the current time. Since the counter-system is operated by an algorithm 32 on the user-inaccessible smart card 3, it can be prevented that the user can change the basic behaviour of the counter-system 22 or to tamper with the time kept.

In the implementation of the method of the invention shown in figure 1, the smart card 3 is provided with algorithms 31-33 for offering a clock functionality on the smart card 3. For the time thus provided, authenticity and trustability can be ensured, firstly due to the nature (identity and integrity) of the smart card 3 itself and secondly due to the use of a trusted time server 1. Optionally, the trustability can be enhanced by encryption/decryption algorithms, which may also be implemented on the smart card 3. Typically also application related logics are implemented, such as, but not exclusively, validation based on the number of prepaid time stamps available on the card or the identity of the user.

The time synchronization algorithm 31 is provided for operating the gateway 21 and requesting the synchronisation time from the time server. The retrieved time value is stored in the memory of the smart card as a reference time point REF_Time. Based on the gateway 21 and time server 1 technology, different synchronisation algorithms 31 are to be used. Examples of such mechanisms are, but not exclusively, retrieving the SMS-C time by means of sending SMS from the device 2 to the device 2 (source = destination), or by implementing NTP (Network Time Protocol) in the case where TCP/IP connection with TTA is available (e.g. PC). Authentication and encryption techniques between the time server and the time synchronisation algorithm, typically by using public-private key encryption, are to be implemented on this level if it is required by end user or target application. Additionally, the synchronisation events can be logged in the protected part of the memory of the smart card.

The time keeping algorithm 32 is provided for keeping track of the elapsed time, based on the reference time REF_Time offered by the time synchronization mechanism and based on the counter-

system offered by the device. By means of the elapsed time and the reference time, the current or present time can be determined.

The time stamping algorithm 33 calculates the current time value and forwards it to the target application 4, 5 or 6. Since the value is determined virtually only by means of the smart card 3, without interaction with the user, identity and integrity can be assured. Authentication and encryption techniques, typically by public-private key encryption, are to be implemented on this level if it is required by end user or target application. Both user authentication (e.g. a private key associated to the user of the service) as well as service authentication (e.g. a private key associated with the time stamping service itself) can be implemented. Additionally, tokens can be generated by the time stamping algorithm 33. Tokens are generated by adding a time stamp to a given value, which can be any relevant piece of information like, but not exclusively, a hash value which is calculated and passed on to the time stamping algorithm 33 by the application 4, 5 or 6 or alternatively generated by the time stamping algorithm itself. In the token generated by the time stamping algorithm, also location information (if available) and identification information can be embedded. The time stamping algorithm 33 can be further provided with one or more of the following: validation-logics, such as for example the functionality based on the available number of prepaid stamps or the identity of the user; monitoring services for enabling the trusted device to monitor the status of external time variables; logging functionality for enabling the keeping of a log file, which can be consulted by the application 4, 5 or 6 and published or changed depending on the authorisation of the user.

The target application 4, 5, 6, to which the present time calculated by the time stamping algorithm 33 is outputted, can run on the smart card 3 itself, on the device 2 or can even be an external application 6 which uses the device 2 as an interface to the smart card 3. Examples of such applications are, but not exclusively, a midlet running on a J2ME enabled GSM cellular phone the interfaces with the SIM card or a PC based application. In other words, when applied to the SIM card of a standard GSM mobile phone, the method of figure 1 turns this phone into a device which can for example offer the possibility to generate a token and to save or send data together with that token.

The time synchronization algorithm 31 which is shown in detail in figure 2 comprises the following steps:

- (311) Get TS_Time (Time Server – Time) from the time server. The time received from the time server 1 through the gateway 21 is the synchronisation time. It can be the result of one or multiple interrogations. Depending on the type of time server 1 or the nature of the gateway 21, this time value TS_Time can have different accuracy, format and reference. Authentication and encryption techniques are to be implemented on this level if it is required by end user or target application.
- (312) Check the accuracy of the received time. The level of accuracy typically depends on the requirements of the target application or the end user. Depending on the type of time server 1 or the nature of the gateway 21, the accuracy check will be done differently.
- (313) If the accuracy check fails, an alternative procedure has to be followed, such as for example to try again a few times or to stop the synchronisation process.
- (314) Set REF_Time based on TS_Time value. The reference time REF_Time is determined and stored in the memory of the smart card 3. The determination of the reference time depends on the type of time server 1 used or the nature of the gateway 21. The reference time is determined on the basis of the synchronisation time. The reference time may have the same format as the synchronisation time if the latter is supplied in the desired format, but the formats may also differ so that a conversion is performed. The desired format of the reference time REF_Time depends on the needs of the target application and end user. Typically the reference time REF_Time is stored as UTC (Coordinated Universal Time). Depending on the format of the time offered by the time server 1, it might be that DST (Daylight Saving Time) and time zone adjustments are needed.
- (315) Start counter A on the device (Lifetime = X). The counter A of the device, which has a lifetime or duration of X, is started in this step, for counting the elapsed time with respect to the reference time.

- (316) Start timer (or counter) B on the device (Lifetime < X). Simultaneously with counter A, a second timer or counter B is started. A second counter is used in case no timer is available. This second timer or counter B has a shorter lifetime than counter A and serves to determine when counter A is about to expire. Upon expiry of timer/counter B, a timer expiration notification is given to smart card 3, so that the appropriate actions can be taken to ensure that the elapsed time is not lost.

The time keeping algorithm 32 is shown in figure 3 and comprises the following steps:

- (321) The expiration notification, generated by timer or counter B, triggers the accuracy-update process or, in the case where the counter A has limited lifetime, the expiration-update process.
- (322) Accuracy-update. Based on the accuracy requirements of the target application or end user and based on the long term accuracy offered by the counter-system on the device, the decision will be made to restart the time synchronisation algorithm 31 in order to renew the reference time REF_Time and reset the counter-system 22 on the device 2, or to update the reference time REF_Time. Typically, when counter A reaches a certain value or when the expiration-update process 323 has been done a given number of times, an accuracy update is desirable to ensure the accuracy of the time offered by the smart card 3. The value at which timer/counter B issues the expiration notification depends on the accuracy of the counter system 22 itself and on the needs of the target application or end user.
- (323) Expiration-update. If counter A has a limited lifetime, there is a need to adjust the reference time REF_Time and reset the counter-system 22.
- (3231) Set ElapsedTime = f (Get counter A). The time passed since the synchronisation or the last expiration update is calculated by means of the value on counter A. This is assumed to be a very good estimation of the time passed since the last adjustment of the reference time REF-Time.

- (3232) REF_Time = REF_Time + ElapsedTime. The reference time is updated, by adding the elapsed time to the previous value of the reference time.
- (3233) Start counter A (Lifetime = X) and (3234) Start timer/counter B (Lifetime <X) on the device. Counter A and timer/counter B are restarted for keeping track of the elapsed time after the update.

The time algorithm 33, shown in detail in figure 4, which calculates the present time and offers it to the device 2, comprises the following steps:

- (331) Request Time from device. The smart card 3 offers the current or present time value upon occurrence of a request on the device.
- (332) Validation. The time request is optionally checked for validity, i.e. whether the processing of the request can be allowed. The validity can be based on authorisation of the application or end user generating the request. Validation can further be based on the number of prepaid stamps available on the smart card 3 or the identity of the user.
- (333) Set ElapsedTime = f (Get counter A). The time passed since the synchronisation or the last expiration update is calculated by means of the value on counter A.
- (334) Time = REF_Time + ElapsedTime. The current time value, "Time" is calculated from the reference time and the elapsed time.
- (335) Authentication and encryption techniques are to be implemented on this level if it is required by end user or target application.

In the following, the scheme of figure 1 will be explained for the particular case where the device 2 is a GSM mobile phone (ME), the smart card 3 is a Subscriber Identity Module (SIM) card and the time server 1 is the Short Message Service Center (SMS-C) of the wireless operator.

The SMS-C functions for storing and forwarding SMS messages. In this process, the center adds a timestamp to the SMS that can be read by the receiver. It is this timestamp that can be used according to the invention for retrieving the synchronization time TS_Time.

The device 2 is any phase2+ enabled GSM mobile phone. The gateway 21 functionality is present on the mobile phone 2, because

the SIM can interact with the ME by protocols that are publicly available and published by ETSI. For this application, focus is on the layers described in the ETSI specifications GSM-11.11 and GSM-11.14. The latter is commonly referred to as SIM Toolkit (STK). STK typically allows the phone 2 to give control to the SIM card 3. This enables applications on the SIM card 3 to interact with the user or the network, for example for customising the display, sending and receiving information by means of Short Message Service (SMS), saving data on the SIM and establishing voice or data connections. STK describes a high level protocol and is available on all Phase2+ enabled ME's.

Each Phase2+ enabled mobile phone 2 offers a set of counters 22, with the following properties: they can be started, deactivated and the current value can be read. Different counters can be managed in parallel, and the duration can be set between 1 second and 24 hours. The SIM is notified upon expiration of the counter. Note: In the STK, the word "timer" is used. Since timers actually do not support ability to read the current value, it is preferred to use the word "counter".

The SIM card 3 is provided with a time synchronisation algorithm 31, a time keeping algorithm 32 and a time algorithm 33. The time synchronization algorithm 31 comprises the sending of an SMS from the phone 2 to the same phone 2. By using the data download feature, the SMS is routed to the SIM card 3, as such enabling the algorithm on the SIM card to read the synchronisation time TS_Time embedded in this SMS. The time synchronisation process 31 is initiated automatically each time the mobile phone 2 is activated or as a result of the accuracy-update (322).

The synchronisation time TS_Time (311) is the time embedded in the received SMS, added to this SMS by the SMS-C when it was processed by the SMS-C. Which SMS-C to use for time synchronisation can be set optionally as a system parameter. If not, the one defined by the mobile phone 2 is used. The TS_Time represents the time local to the SMS-C. It includes the Time Zone value, indicating the difference between the local time and GMT. The Time Zone value enables the algorithm on the SIM card to calculate the equivalent time in GMT if necessary (314) or perform other similar calculations as required by the target application. The Time Zone value takes into account daylight saving time (DST), such that when the sending mobile phone 2 changes

from regular (winter) time to daylight saving (summer) time, there is a change in Time Zone value.

The accuracy check (312) is done by starting a counter C on the phone 2 once the message is sent and to read the value of counter C once the same SMS is received. This value of counter C represents the travel time of the SMS, between its departure and arrival. If this value is less that a predefined value, the TS_Time is accepted for further processing. This predefined value is a system parameter and kept on the SIM card. If the value of counter C, i.e. the travel time is above or equal to the predefined value the synchronisation process stops and an alternative procedure (313) is started, which may for example comprise displaying an error message, so that it can be indicated to the user that he has to reset his phone by switching it off and back on.

The reference time REF_Time is derived from the synchronisation time TS_Time (314). The value of counter C is divided by 2 and the result is added to the TS_Time, so that the travel time of the SMS is taken into account. The DST flag is adjusted: it is set to 0 if the current REF_Time was generated during winter time and to 1 during summer time.

Counter A is started (315) on the mobile phone 2, with maximum lifetime of 24 hours. Simultaneously, counter B is started (316) on the phone 2 with lifetime of 23 hours. The expiration notification 321 is generated by counter B.

In the time keeping algorithm 32, the accuracy-update 322, which is performed on receipt of the expiration notification 321: The time synchronization algorithm 31 is re-activated automatically when the expiration-update 323 has occurred a given amount of times. This amount is a system parameter.

For the expiration-update 323, since counter A has a limited lifetime, there is a need to adjust the REF_Time and reset the counter-system 22. The ElapsedTime is the current value of counter A (3231). The new REF_Time is set to the previous REF_Time + ElapsedTime (3232) and the counters A and B are restarted (3233 and 3234).

The time algorithm 33 is started on occurrence of a time request 331 on the phone 2. This request can be generated by an

application, automatically or by user request. The application can be formed by any software running on the phone 2 or on the SIM 3 itself. The application can be part of a client server architecture, like, but not exclusively, a web browser.

Validation 332 is done by password. Additionally, alternative billing scenarios can be offered, for example to invoice the SIM card owner by using the SIM ID, or to invoice this service to a third party. In both cases, prepaid functionality can be offered, which means that a certain amount of time stamps can be bought in advance.

For calculating the present time, the elapsed time is retrieved (333) and added to the reference time (334). If needed, an adjustment is made for the DST, based on the DST flag. Optionally, the present time may be encrypted and/or authenticated on the SIM card as well.

An example of an application for which the time obtained by the method of figures 1-4 is suitable is the time registration method of figure 5, in which a time registration algorithm 34 is provided on the smart card 3. This time registration algorithm comprises the following steps:

- (341) Time Registration Request. This occurs for example when the user operates the device 2 when he wants to register a time point. To this end, he selects the time registration application by means of the user interface of the device 2.
- (342) Get Task Reference. The user is asked to input or select a reference to be attached to the time point to be registered. In the case of input, the user is given a text field for inputting an alphanumeric reference. In the case of selection, the user is given a list of task references, which has previously been downloaded to the smart card memory.
- (343) Get Location Info. In the case of a GSM mobile phone, this involves a communication between the phone and the nearest communication mast of the network. This communication is transparent to the user. The location of the phone can be approximated by means of the known location of the mast.
- (344) Get Time. The present time is retrieved by means of the time algorithm 33.

- (345) Encryption and authentication techniques may be implemented here if desired.
- (346) Send time, task reference and location info. The information is sent to a time data collecting unit, where the registered time points are collected. In the case of GSM, the communication is performed by means of SMS.

Claims

1. A method for offering time on a smart card which is provided for being carried in a host device which comprises at least a first time counter and a gateway for communication with a time server, characterised in that the method comprises the step of running an algorithm on a processor of the smart card for performing the following steps:

a) reserving a user-inaccessible memory location on the smart card for storing a time,

b) sending a synchronisation time request via the gateway to the time server and, upon receipt of a reply of the time server, extracting a synchronisation time from the reply and storing the synchronisation time as a reference time on the user-inaccessible memory location,

c) starting the first time counter of the host device for counting an elapsed time with respect to the reference time,

d) upon receipt of a present time request, retrieving the elapsed time from the first time counter, calculating a present time on the smart card by adding the elapsed time to the reference time and outputting the present time.

2. The method of claim 1, characterised in that the method further comprises the steps of encrypting the synchronisation time on the time server and decrypting the retrieved synchronisation time on the smart card.

3. The method of claim 1 or 2, characterised in that the present time is outputted in a time stamp which is generated on the smart card, the time stamp further comprising user-identification data which is stored on the smart card and/or document trustability data supplied by an application running on the host device and/or any other data.

4. The method of claim 3, characterised in that the time stamp is encrypted before being outputted.

5. The method of any one of the claims 1-4, characterised in that the method further comprises the step of performing a validity check on the present time request, before outputting the present time.

6. The method of any one of the claims 1-5, characterised in that the method further comprises the step of, on receipt of the

reply comprising the synchronisation time from the time server, performing an accuracy check on the synchronisation time.

7. The method of any one of the claims 1-6, characterised in that step c) further comprises starting a second time counter of the host device simultaneously with the first time counter for counting the elapsed time with respect to the reference time, the second time counter having a shorter duration than the first time counter, and that the algorithm is further provided for performing the following steps:

e) after lapse of the second time counter, restarting the first time counter,

f) upon restart of the first time counter, calculating a sum by adding the previously elapsed time to the reference time and storing the sum as a new reference time on the user-inaccessible memory location.

8. The method according to any one of the claims 1-7, characterised in that the method further comprises the step of storing a time zone value in the memory of the smart card, the time zone value being determined by means of the synchronisation time, the time zone value being outputted along with the present time.

9. The method according to any one of the claims 1-8, characterised in that the algorithm is further provided for performing the following steps:

g) maintaining a daylight saving time flag in the memory of the smart card, the daylight saving time flag being set to a first value, respectively a second value in correspondence with winter time, respectively summer time,

h) adjusting the present time in function of the daylight saving time flag in step d).

10. The method of any one of the previous claims, characterised in that the gateway of the device is provided for wireless communication with the time server via a wireless communication network and that the synchronisation time is retrieved by means of a wireless communication protocol.

11. The method of claim 10, characterised in that the wireless communication protocol comprises sending an SMS from the device

via the wireless network to a network time server and via the wireless network back to the device.

12. The method of claim 10, characterised in that the wireless communication protocol comprises sending an SMS from the device via the wireless network to a third party time server and sending a return SMS from the third party time server via the wireless network to the device.

13. The method of any one of the claims 1-9, characterised in that the gateway of the device is provided for wired communication with the time server via a wired communication network and that the synchronisation time is retrieved by means of a TCP/IP connection.

14. A method for time registration by means of a mobile telecommunication device, the mobile telecommunication device being provided for hosting a smart card and comprising at least a first time counter and a gateway for communication between the smart card and a time server, the time registration method comprising the step of communicating a present time from the mobile telecommunication device to a time data collecting unit, characterised in that the present time is calculated with the method of any one of the claims 1-13.

15. The method of claim 14, characterised in that the present time is calculated and communicated to the time data collecting unit upon operation of time registration means by the user, the time registration means being provided on the smart card and being operable by the user via a user interface of the mobile telecommunication device.

16. The method of claim 14 or 15, characterised in that in case of absence of connection between the device and the time data collecting unit, the calculated present time is stored on the smart card and communicated to the time data collecting unit once the connection is repaired.

17. The method of any one of the claims 14-16, characterised in that the method further comprises the steps of:

i) providing task referencing means in the time registration means on the smart card, for enabling the user to refer a time point to a task,

j) attaching a user-selected or user-inputted task reference to the present time and communicating the task reference with the present time to the time data collecting unit.

18. The method of claim 17, characterised in that the method further comprises the step of downloading a series of task references to the smart card, which are user-selectable by means of the task referencing means.

19. The method of any one of the claims 14-18, characterised in that the method further comprises the steps of:

k) retrieving location information on the location of the mobile telecommunication device within the communication network,

l) communicating the location information with the present time to the time data collecting unit.

20. The method according to any one of the claims 14-19, characterised in that the present time and the relevant other information is communicated to the time data collecting unit by means of an SMS message.

21. A smart card comprising a memory for storing data and a microprocessor for running algorithms, characterised in that the smart card is embedded with the algorithm of any one of the claims 1-13.

22. The smart card of claim 21, characterised in that the smart card is embedded with a second algorithm for performing the time registration method of any one of the claims 14-19.

23. The smart card of claim 21 or 22, characterised in that the smart card is embedded with an encryption/decryption algorithm.

24. A combination of a smart card according to any one of the claims 21-23 and a device which is provided for hosting a smart card, the device comprising at least a first time counter and a gateway for communication between the smart card and a time server.

Fig. 1

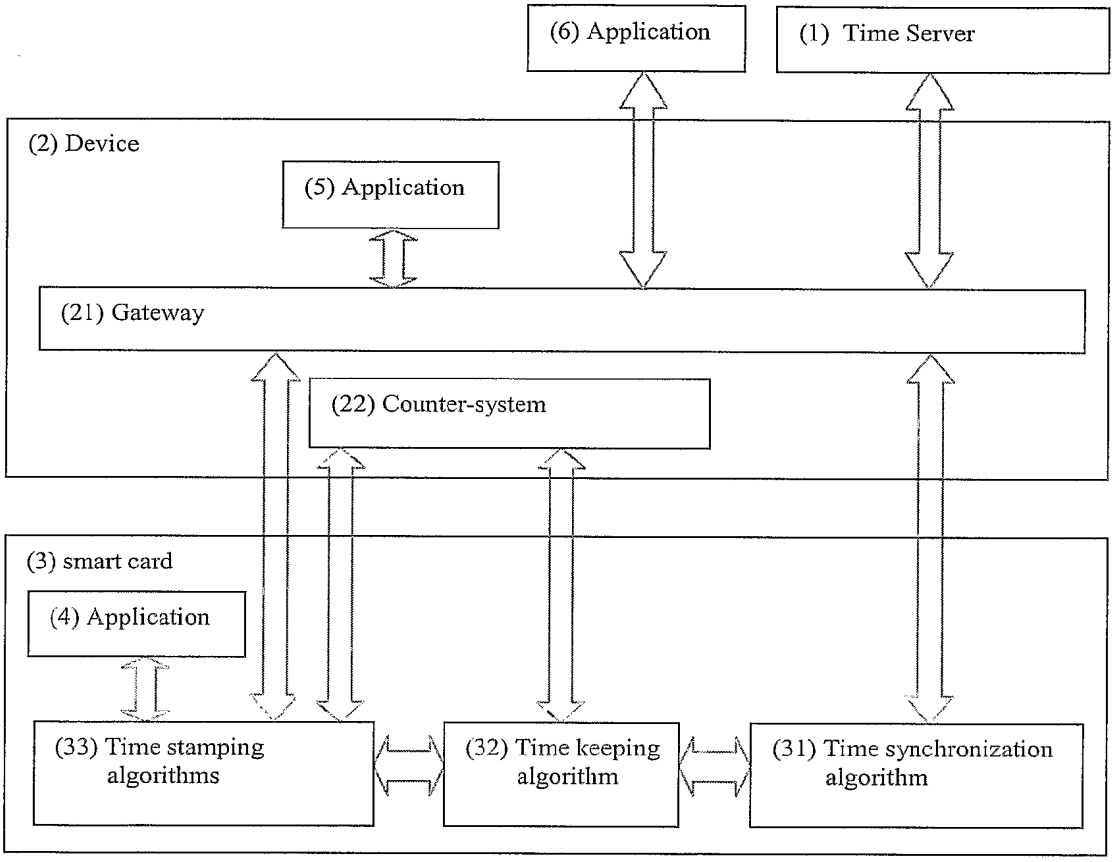

(6) Application
(1) Time Server
(2) Device
(5) Application
(21) Gateway
(22) Counter-system
(3) smart card
(4) Application
(33) Time stamping algorithms
(32) Time keeping algorithm
(31) Time synchronization algorithm

Fig. 2

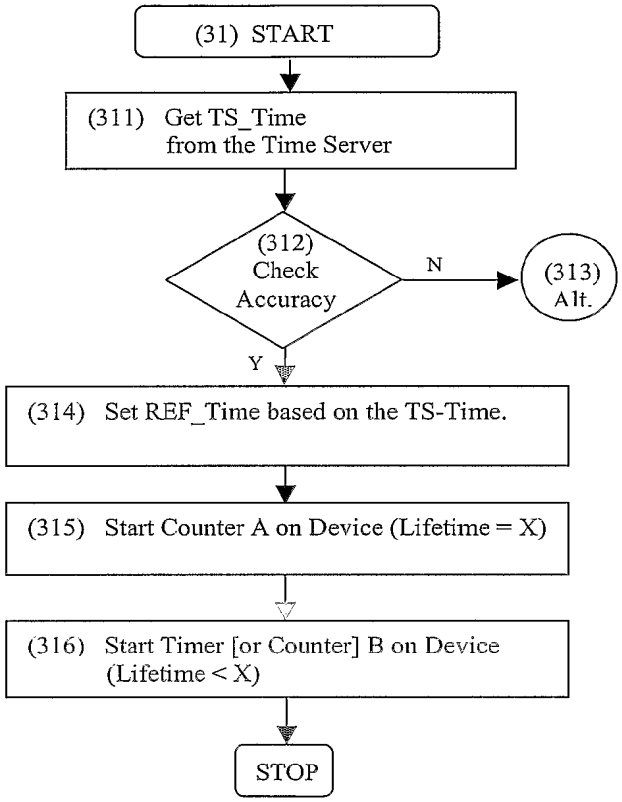

(31) START
(311) Get TS_Time from the Time Server
(312) Check Accuracy
N
(313) Alt.
Y
(314) Set REF_Time based on the TS-Time.
(315) Start Counter A on Device (Lifetime = X)
(316) Start Timer [or Counter] B on Device (Lifetime < X)
STOP

Fig. 3

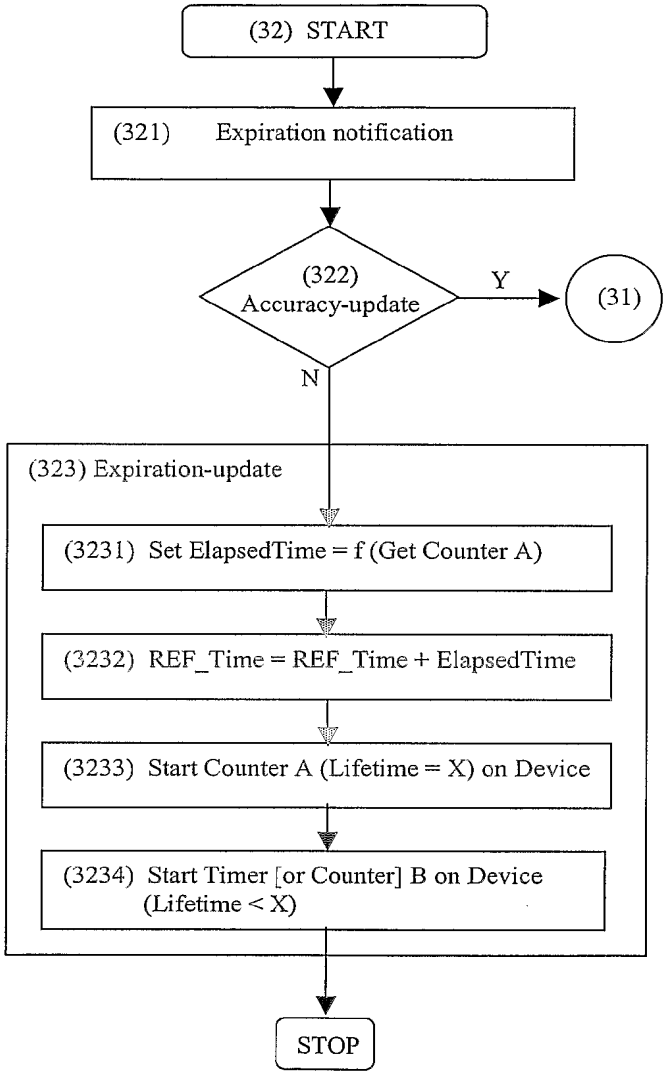

(32) START
(321) Expiration notification
(322) Accuracy-update
Y
(31)
N
(323) Expiration-update
(3231) Set ElapsedTime = f (Get Counter A)
(3232) REF_Time = REF_Time + ElapsedTime
(3233) Start Counter A (Lifetime = X) on Device
(3234) Start Timer [or Counter] B on Device (Lifetime < X)
STOP

Fig. 4

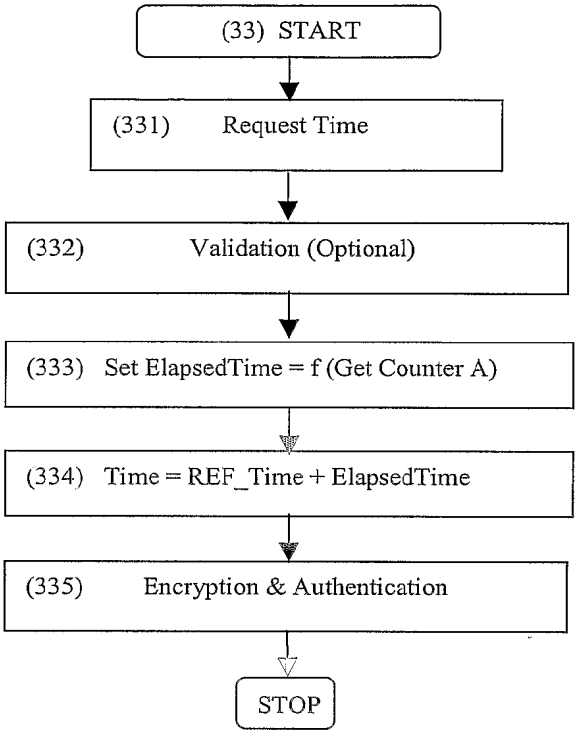
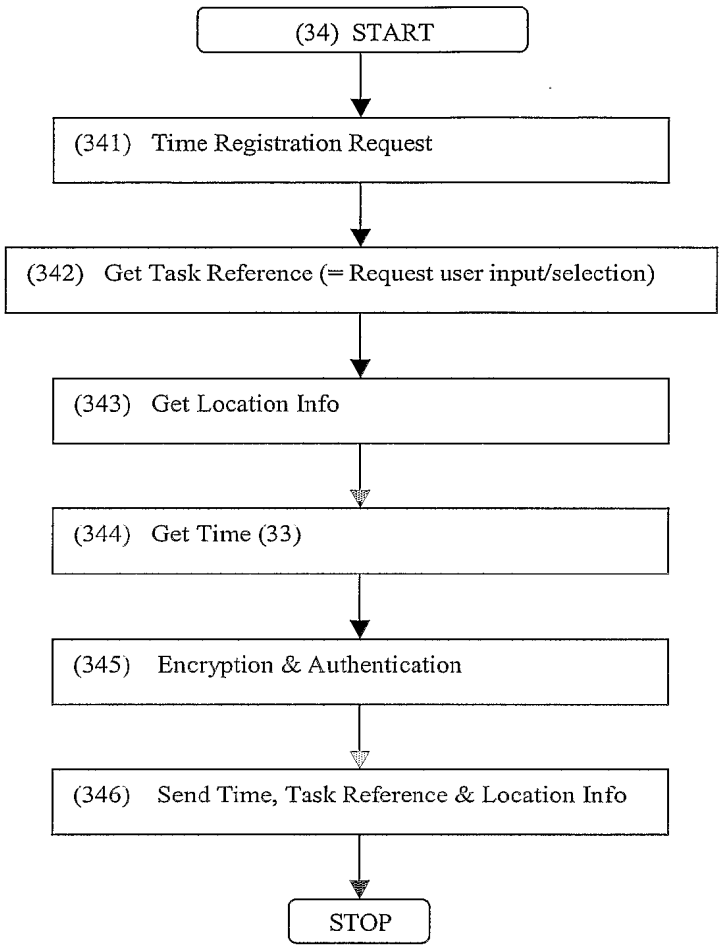

(33) START
(331) Request Time
(332) Validation (Optional)
(333) Set ElapsedTime = f (Get Counter A)
(334) Time = REF_Time + ElapsedTime
(335) Encryption & Authentication
STOP

Fig. 5


(34) START
(341) Time Registration Request
(342) Get Task Reference (= Request user input/selection)
(343) Get Location Info
(344) Get Time (33)
(345) Encryption & Authentication
(346) Send Time, Task Reference & Location Info
STOP

INTERNATIONAL SEARCH REPORT

International Application No
/BE2004/000023

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04M15/00 G06F1/14 H04Q7/32 H04M1/725 G07C1/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G04G H04M H04Q G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99/41919 A (RITTER RUDOLF ;SWISSCOM AG (CH)) 19 August 1999 (1999-08-19) page 2, line 23 - page 3, line 4 page 3, line 28 - line 31 page 4, line 7 - page 5, line 14 page 5, line 24 - page 8, line 6 page 10, line 30 - line 32 page 14, line 28 - page 15, line 2	1-15,21, 23,24
Y		16-20,22
Y	WO 01/37225 A (NOKIA NETWORKS OY ;SAARI JARMO (FI)) 25 May 2001 (2001-05-25) cited in the application abstract; figures page 2, line 1 - line 21	16-20,22

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 July 2004	03/08/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
T/BE2004/000023

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 624 014 A (FISCHER ADDISON M) 9 November 1994 (1994-11-09) abstract; figure 1 column 5, line 25 - column 6, line 17	1
A	US 2002/082992 A1 (RITTER R) 27 June 2002 (2002-06-27) page 1; figures 1,5 paragraph '0004! paragraph '0008! paragraph '0016! paragraph '0026! - paragraph '0033! paragraph '0043!	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
T/BE2004/000023

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 9941919 A	19-08-1999	AT	205352 T	15-09-2001
		AU	2262099 A	30-08-1999
		WO	9941919 A2	19-08-1999
		DE	59900243 D1	11-10-2001
		EP	1057350 A2	06-12-2000
		US	6543686 B1	08-04-2003
WO 0137225 A	25-05-2001	FI	992449 A	16-05-2001
		AU	1527001 A	30-05-2001
		EP	1232484 A1	21-08-2002
		WO	0137225 A1	25-05-2001
EP 0624014 A	09-11-1994	US	5422953 A	06-06-1995
		AT	196582 T	15-10-2000
		AT	205309 T	15-09-2001
		AU	666424 B2	08-02-1996
		AU	5778194 A	17-11-1994
		CA	2120665 A1	06-11-1994
		DE	69425923 D1	26-10-2000
		DE	69425923 T2	18-01-2001
		DE	69428215 D1	11-10-2001
		DE	69428215 T2	18-04-2002
		DK	624014 T3	04-12-2000
		EP	0624014 A2	09-11-1994
		EP	0770953 A2	02-05-1997
		EP	0841604 A2	13-05-1998
		ES	2149843 T3	16-11-2000
		GR	3034459 T3	29-12-2000
		JP	7254897 A	03-10-1995
		PT	624014 T	29-12-2000
		US	2003041246 A1	27-02-2003
		US	6408388 B1	18-06-2002
		US	5936149 A	10-08-1999
US 2002082992 A1	27-06-2002	WO	0059243 A1	05-10-2000
		AT	243403 T	15-07-2003
		AU	2824299 A	16-10-2000
		DE	59906044 D1	24-07-2003
		EP	1326456 A2	09-07-2003
		EP	1326457 A2	09-07-2003
		EP	1166577 A1	02-01-2002
		ES	2201678 T3	16-03-2004
		JP	2002540744 T	26-11-2002